UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

INFORMATION ASSOCIATED WITH MICROSOFT EMAIL ADDRESS ATTORNEYGRAHAM@HOTMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY MICROSOFT, SEE ATTACHMENT A-2

Case No. 18-M-1239

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

INFORMATION ASSOCIATED WITH MICROSOFT EMAIL ADDRESS ATTORNEYGRAHAM@HOTMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY MICROSOFT, SEE ATTACHMENT A-2

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B-2

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: 18 U.S.C. §§ 1343 and 1349

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

C.J. Sebero, FBI Special Agent
Printed Name and Title

Sworn to before me and signed in my presence:

Date: 4/2/18

Judge's signature

City and State: Milwaukee, Wisconsin

William E. Duffin, U.S. Magistrate Judge
Printed Name and Title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, C.J. Sebero, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises controlled by Google, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043 and Microsoft, an email provider headquartered at One Microsoft Way, Redmond, WA 98052. The information to be searched is described in the following paragraphs and in Attachments A-1 and A-2. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google and Microsoft to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachments B-1 and B-2. Upon receipt of the information described in Section I of Attachments B-1 and B-2, government-authorized persons will review that information to locate the items described in Section II of Attachments B-1 and B-2.

2. I have been a Special Agent with the Federal Bureau of Investigation since 2016. My duties as a Special Agent include investigating violations of federal law, including various white-collar crimes such as wire fraud, mortgage fraud, and money laundering. I have received training regarding investigating white-collar crimes, I have participated in numerous investigations of white-collar crimes, and I have served as the affiant for applications for search warrants.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that the information associated with the accounts identified in Attachments A-1 and A-2 contain fruits, evidence, and instrumentalities related to violations of 18 U.S.C. §§ 1343 and 1349 (the "Subject Offenses"), as further described in Attachments B-1 and B-2.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. Michael Krill, and individuals going by the names Eric Murray, Wanda Collier, Harvey Graham, Naomi Ratinov, and others unknown to law enforcement perpetrated a scheme to defraud clients and associates out of funds the victims believed they were investing in lucrative international financial transactions.

7. Krill, Murray, Collier, Graham, and Ratinov recruited victims to these transactions by describing the transactions orally and by email; by sending by email to the victims putative supporting documents associated with the deals; and by directing victims orally and by email to send money to particular accounts chosen by the fraudsters.

8. The underlying financial transactions and supporting documents at issue appear to be complete fabrications.

9. Based on interviews with witnesses and the review of emails and other documents recovered during the execution of a search warrant at Krill's home and office, Krill, Murray,

Collier, Graham, Ratinov and others advised victims by email and other means that Murray and Krill could facilitate the victims' participation in an investment opportunity: if investors paid an initial investment of funds into Krill's law firm's JP Morgan Chase trust account ("IOLTA"), those funds would be used to pay fees to facilitate multi-million dollar bank transfers, and the investors would then receive as profit, a portion of that bank transfer in an amount many times greater than their initial investment.

10. Krill told victims by office phone, cell phone, in person, and by email, that the transactions would benefit and be facilitated by a man in New York named Eric Murray or his business, "Unite2Jam." For certain deals, the transactions would also be facilitated by an individual who claimed to be a lawyer in England, variously identified as "Harvey Graham" or "Graham Harvey" and various bankers and other intermediaries inside and outside the United States. Those intermediaries, who corresponded directly by email and indirectly through their co-actors by email with victims, included a woman named Wanda Collier and another woman named Naomi Ratinov. Krill, Murray, Collier, Graham, and Ratinov communicated with victims and one another by email.

11. As a result of these representations, Krill received transfers from victims totaling hundreds of thousands of dollars. Krill stated to victims that Krill then sent money from his IOLTA law firm trust account to accounts of Harvey Graham and other deal facilitators at various banks in the United States and United Kingdom including Barclays, Royal Bank of Scotland, and NatWest Bank purportedly to pay for certificates, insurance bonds, anti-money laundering certificates, and anti-fraud certificates.

12. Trust account records show that Krill instead transferred funds paid into his IOLTA by victims to individuals and entities unrelated to the purported international financial transactions into which his victims believed they were investing.

13. Krill also kept much of the money transferred into his IOLTA for himself. He often wrote himself checks on the same day he received a transfer from a victim and ultimately wrote checks to himself from his JP Morgan Chase IOLTA totaling nearly $200,000 between 5/2/2015 and 8/30/2016.

I. Evidence of the Scheme to Defraud

A. Interviews with Victim-Witnesses

i. Dean R. Rossey

14. Dean Rossey was interviewed at the United States Attorney's Office on September 2, 2016 in the presence of his attorney, Patrick Roney.

15. In May 2014, Krill recruited Rossey into a business deal in which Rossey would initially make a payment through Krill's IOLTA of $25,000 in exchange for the right to a $350,000 share of a $16.2 million payment from an entity in China. Krill and Murray told Rossey that Rossey's investment was necessary to pay for a "certificate" that was required to bring the Chinese money to the United States.

16. Krill and Murray told Rossey that all certificates had to be paid through Murray and his company "Unite2Jam."

17. Krill instructed Rossey to wire the $25,000 to Krill's IOLTA account. Rossey wired the funds from his Wells Fargo account to the Krill IOLTA account.

18. Krill successfully solicited additional payments from Rossey to pay what Krill represented were "additional fees" for that transaction totaling approximately $70,000.

19. Krill successfully solicited Rossey's participation in a similar transaction apparently based in the United Kingdom, and Rossey invested through Krill approximately $25,000 in that deal.

20. Trust account records show that Rossey has paid over $150,000 to Krill.

21. Rossey stated that he has participated in conference calls with both Krill and a person who represented himself as Eric Murray. Rossey never met Murray in person.

22. Murray and Krill represented to Rossey that a British solicitor named Graham Harvey (or "Harvey Graham") was integral to the financial transaction. It is unclear whether any such person exists, but an email address, "attorneygraham@hotmail.com", was often used to perpetrate the fraud and send emails that were forwarded to victims. The physical address provided by Krill to Rossey for Graham Harvey is not real. Information obtained from British law enforcement sources indicates that there is no solicitor registered in the United Kingdom under Harvey Graham and Graham Harvey is not associated with Krill or Murray. According to http://harveyassociates.co.uk/ Harvey Associates are aware that a fraud had occurred using the name "Harvey" and confirm that they are not part of the nefarious fraudulent activity.

23. On June 24, 2014, Krill emailed Rossey and attached what he stated was "a copy of the Inland Revenue Certificate which requires a payment of $16,500 to release the $10,500,000 and a confirmation of the wire. Eric [Murray] has $2,500 to invest in this transaction. He needs $14,000 to complete. For this investment, you will be paid $500,000. My investment to date is $30,000. I have been working on this transaction for two months. Paulinus Blair is the banker in London that Eric [Murray] is working with to get this transaction completed. I just got off the phone with him. Mr. Paulinus confirmed that the $10,500,000.00 wire will be released by Suntrust

Bank in the US within 24 hours of receipt of the certificate." The attached "Letter of Guarantee" is facially illegitimate and riddled with typographical errors.

24. Rossey and his wife called a bank in the United Kingdom that Krill represented to Rossey was arranging one of the transactions in which Rossey believed he had invested, and the assistant to the banker listed on the certificate provided by Krill confirmed the banker had never heard of Eric Murray or Unite2Jam.

25. Rossey stated that he never received any of the large payments he was promised in return for his investments.

ii. William A. Patch

26. William A. Patch was interviewed at the United States Attorney's Office on September 2, 2016.

27. Patch has known Krill for between 25 and 30 years and has employed Krill as an attorney for Patch's real estate development company.

28. Krill recruited Patch into a business deal in which Patch would initially make a payment to Eric Murray through Krill of $7,500. Patch wired those funds from his account to Krill's IOLTA. Patch made the payment to Krill from a BMO Harris account. Murray told Patch that Patch would shortly receive $250,000 in return for his $7,500 investment.

29. Krill put Patch in telephone and email contact with a person representing himself to be Eric Murray, but Patch never met Murray in person.

30. Murray also told Patch by phone and email that Patch would later receive a $30 million investment from Murray in exchange for additional payments.

31. Murray and Krill attempted to recruit Patch into multiple "deals" Murray said he was working on including: (a) a $16.2 million deal with NatWest Bank; and (b) an $18 million

deal involving Barclays that, in turn, morphed into a third deal that involved $9 million that would be paid through Barclays and $9 million that would be paid by the "Saudi British Bank."

32. Patch believed he has paid between $200,000 and $225,000 to Krill's IOLTA in order to "invest" in these schemes.

33. Patch dealt with Murray directly and through Krill.

34. Patch stated that he never received any of the large payments he was promised in return for his investments.

B. Documents from Other Victim-Witnesses

35. In May 2016, Rafael Gavioli provided to the Supreme Court of Wisconsin's Office of Lawyer Regulation documents, including emails and email attachments, supporting his claim that he had been defrauded by Krill. The schemes described by Gavioli are consistent with those described by the witnesses whose interviews are summarized herein.

36. On September 25, 2015, Gavioli signed an agreement with Murray stating that Gavioli would loan Murray $17,500 to enable Murray to receive a $16,200,000 "international private banking transaction." Murray would then pay Gavioli the $17,500 he loaned Murray and an additional $55,000 in interest within 14 days. The agreement states above Michael M. Krill's signature that "the undersigned acknowledges that he is the attorney representing the Borrower [Murray] and hereby confirms that the representations and documentation made herein are true and correct."

37. Gavioli states that he made the $17,500 loan called for by the agreement but never received any of the promised payments.

C. Preliminary Financial Analysis of Krill's IOLTA Transactions

38. An FBI Forensic Accountant performed a preliminary analysis of Krill's JPMorgan Chase IOLTA transactions between May 1, 2015 and August 30, 2016. This analysis revealed many transactions that are inconsistent with the investment arrangements Krill pitched to his victims.

a. On May 28, 2015, Dean Rossey deposited $17,900 into Krill's IOLTA account. The same day, Krill wired from that account $17,800 to "Pey Tradders Ltd.," an entity with no known affiliation with the international financial transaction into which Rossey was told he was investing.

b. On June 17, 2015, Rossey's company "Horizon Enterprises LLC" wired $43,000 into Krill's IOLTA. On June 18, 2015, Krill wired $38,000 from that account to "Pey Tradders Ltd.," an entity with no known affiliation with the international financial transaction into which Rossey was told he was investing.

c. On July 20, 2015, Rossey's company "Horizon Enterprises LLC" wired $40,000 into Krill's IOLTA account. That same day, Krill wired from that account $40,000 to "Optra Sales and Services Ltd," an entity with no known affiliation with the international financial transaction into which Rossey was told he was investing.

d. On September 4, 2015, Rossey wired $24,000 into Krill's IOLTA account, and Patch's Company "First Pain Care LLC" wired $20,000 into Krill's IOLTA account. The same day, Krill wired $39,000 to "M. U. Ndukwe," a person with no known affiliation with the international financial transaction into which Rossey and Patch were told they were investing.

39. Krill wrote a March 30, 2016 letter to the Supreme Court of Wisconsin Office of Lawyer Regulation stating that he "verified all of the information that was delivered to Mr. Gavioli as being true and correct." The Gavioli documents, as described above, included frauds and forgeries.

D. The use of email to perpetrate the fraud

40. In July 2017, a search warrant was executed at Krill's home and office. Thousands of documents were seized, including a very large number of emails between Krill, Murray, Collier, Ratinov, and Graham in furtherance of the fraud scheme described here.

41. The victims were provided with documents, often via email, concerning the purported international money transfers, and many of those documents are inconsistent with each other with respect to the banks involved, locations of the banks, countries involved, and amounts to be transferred.

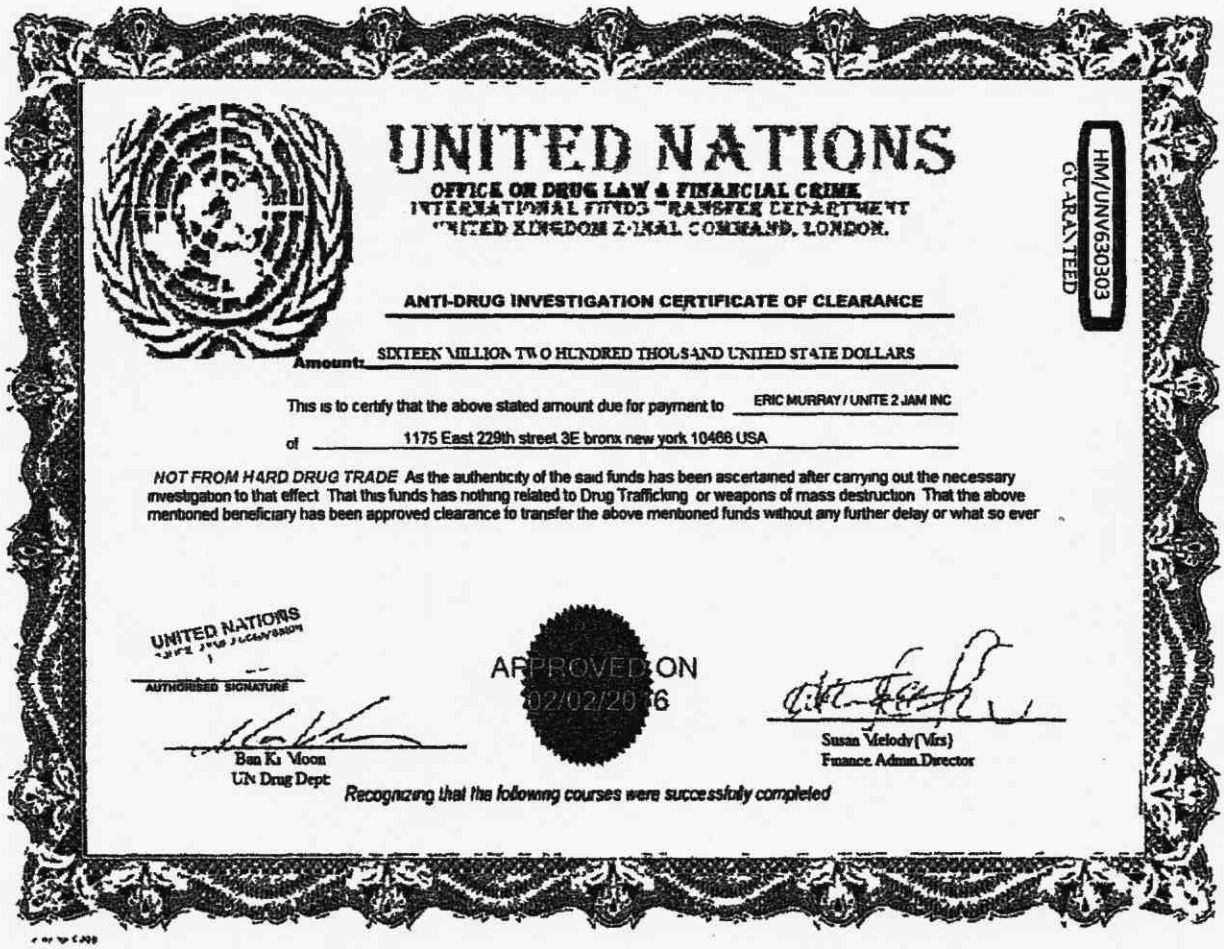
i. Eric Murray email

42. Eric Murray used email addresses unite2jaminc@gmail.com and unityjamii@gmail.com to perpetrate a scheme to defraud various victims. Hundreds of emails from Murray were sent to his co-actors (Krill, Collier, Ratinov, Harvey Graham and others) and to his victims and were typically sent from "unite2jaminc@gmail.com".

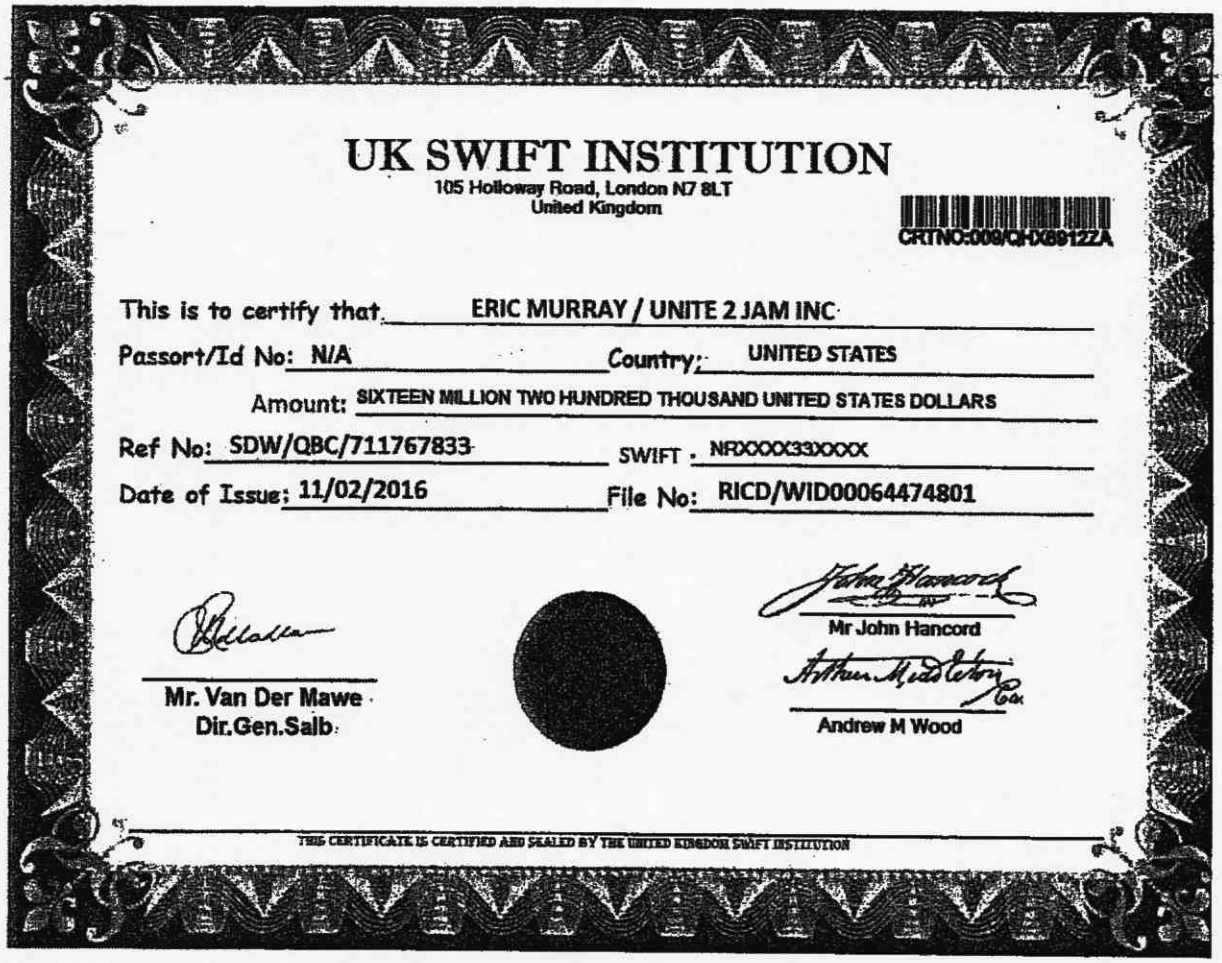
43. On January 29, 2015, Murray wrote an email addressed to "admin@nateweste@uk.com" and "attorneygraham@hotmail.com", copying Krill and Collier, which stated "I MEAN MY NEW EMAIL IS unite2jaminc@gmail.com". He also stated "unityjamii@gmail.com" was another email address of his.

44. Both "unite2jaminc@gmail.com" and "unityjamii@gmai.com" were listed in Murray's email signature block on dozens of emails furthering the fraud scheme.

45. For example, Murray emailed to Rossey and Krill from the email address "unite2jaminc@gmail.com" on February 2, 2016. A document he attached to that email purporting to support one of the international financial transactions appears to be a manipulated course completion certificate and states on the bottom of the image: "Recognizing that the following courses were successfully completed." It also purports to have been signed by "Ban Ki Moon," of the "UN Drug Dept." Ban Ki Moon was the Secretary-General of the United Nations.



46. Other documents emailed to Rossey from Murray's unite2jaminc@gmail.com address supporting the purported underlying international financial transactions are rife with facial absurdities including, for example, signatures of John Hancock and Arthur Middleton copied from the Declaration of Independence.



UK SWIFT INSTITUTION

105 Holloway Road, London N7 8LT
United Kingdom

CRTNO:009/QH-DX89122A

This is to certify that ERIC MURRAY / UNITE 2 JAM INC

Passort/Id No: N/A Country: UNITED STATES

Amount: SIXTEEN MILLION TWO HUNDRED THOUSAND UNITED STATES DOLLARS

Ref No: SDW/QBC/711767833 SWIFT : NRXXXX33XXXX

Date of Issue: 11/02/2016 File No: RICD/WID00064474801

Mr. Van Der Mawe
Dir.Gen.Salb

Mr John Hancord

Andrew M Wood

THIS CERTIFICATE IS CERTIFIED AND SEALED BY THE UNITED KINGDOM SWIFT INSTITUTION

47. On December 11, 2015, Murray, from email address "unite2jaminc@gmail.com", and Michael Krill corresponded by email in order to craft a message that Murray, from "unite2jaminc@gmail.com", ultimately sent to a victim, Gerry Klamrowski. In order to entice Klamrowski to continue to send "loans" to Krill and Murray, Murray promised by email that he would give Klamrowski a loan of "$1,000,000." Klamrowski ultimately wired to Krill and Murray over $100,000.

48. Krill and Murray told Rossey that a banker at the Royal Bank of Scotland named Michael Burrows was organizing one of the financial transactions in which Rossey invested. In April 2016, Andrew Carter, Head of Quality & Control at NatWest Bank confirmed via email to Dean Rossey's wife, Zulima Rossey, that no one affiliated with that bank and named Michael

Burrows was involved in any such transaction. Carter also confirmed that a document that Murray sent to Rossey from email address "unite2jaminc@gmail.com" purportedly confirming the transaction was "NOT genuine."

ii. Wanda Collier email

49. Wanda Collier used the email account: "jonesvillerealtyfinance@gmail.com".

50. Wanda Collier emailed with Krill, Murray, victims, and others to entice victims to send money to her and to other fraudsters.

51. On August 6, 2014, Murray wrote to Rossey and Krill stating that a payment of $3,300 to "our Wells Fargo Account" was necessary in order to have funds "released." The Wells Fargo account he then indicates is an account associated with "Jonesville Realty & Financial Services, Inc." – an entity affiliated with Wanda Collier.

52. In September 2014, Murray directed Rossey to send Collier $14,000 via Krill's IOLTA. Krill prepared a contract that Murray sent to Rossey. The contract states that upon receiving the $14,000, Collier "will immediately transfer the $14,000 to a designated bank in England where said amount shall be immediately paid to Inland Revenue Services to cause the release of the [$10,500,000.00] Loan . . . Murray and Collie represent to Rossey that upon payment of the $14,000.00 investment by Rossey and receipt of the payment from Inland Revenue Services, the Bank of England shall issue a telex to the Federal Reserve" and Rossey would receive $500,000.

53. On September 1, 2015, Murray emailed Patch and Krill regarding a fraudulent Saudi British Bank deal. A fabricated financial document that was attached listed Murray as the potential beneficiary of a $10,500,000 payment via a Sun Trust Bank account (number *1864) with Beneficiary's Account Name "Jonesville Realty and Financial Services Inc."

54. On January 14, 2016, Collier emailed Murray a document entitled "TMC Retainer Fee Schedule (2016) that Murray then sent to Krill, Rossey, and Patch, and the body of Murray's email stated "This is a $100,000,000 plan for all our projects please read below this sentence. And please open the attachment below."

55. On May 28, 2015, Collier emailed Murray, copying Krill, Rossey, and Patch with the subject line "$6.00 ,in bank" and attaching an email indicating that Murray was "pursuing additional funds" to complete their various fraudulent deals.

iii. Naomi Ratinov email

56. Ratinov used the email account "Paradise.quest.sm52@gmail.com".

57. Ratinov appears to have worked with Murray to conjure and document the deals that were ultimately pitched to victims.

58. On March 3, 2015, Krill sent an email to Murray and Patch attaching an earlier email exchange between Murray and Ratinov (from address "paradise.quest.sm52@gmail.com"). In the earlier exchange, Ratinov stated that $7,000 was necessary to gain access to $100 million in "British gilt bonds" that were "currently being held in Renaissance capital investment bank in Moscow. The $100m payable in tranches will be paid from their sister branch Renaissance capital. Those fund are in deutsche bank New York, New York. The name of the Company Renaissance Capital. My name is Naomi Ratinov. The asset are British gilt bonds valued at $100 million. Naomi." Attached to the March 3, 2015 email was a putative loan agreement indicating that Patch would loan Murray $25,000 by sending $25,000 to Krill. That $25,000 would then be used by "Harvey Graham" to complete a "Private Banking Transaction" that would cause $16.2 million to be wired to Murray, who would then immediately invest over $2 million, and

ultimately invest $30 million, into companies owned by Patch. No such "International Banking Transaction" ever occurred, and no such loan was ever made to Patch or his companies.

59. On March 4, 2015, Murray forwarded to Krill and Rossey an email from Ratinov stating that she had signed a loan agreement. The agreement was attached and indicated that a lender, "Naomi Ratinov and her company Paradise Quest, Inc." would be paid $7,500 via a bank account, the details of which were given in the agreement. Rossey was listed as the "investor" and Murray and Krill were listed as "Partners." As "consideration for the $7,500 loan," Rossey was to be paid "$1,500,000.00." Rossey never received that payment.

iv. Harvey Graham email

60. Graham used the email address "attorneygraham@hotmail.com".

61. On July 18, 2016, "HarveyGraham Solicitors Co", from email address "attorneygraham@hotmail.com", emailed Krill and copied Murray (at "unite2jaminc@gmail.com") with bank account information. Krill printed that email and annotated it with handwritten notes including "7,100.00 – Dean".

62. On July 20, 2015, Harvey Graham emailed Murray with bank account information listing "Optra Sales and Services" as the account name. On July 20, 2015, Murray forwarded that same email to Krill. On that same day, Dean Rossey wired $40,000 to Krill's IOLTA and Krill wired from his IOLTA $40,000 to the Optra Sales account provided by Harvey Graham and Murray. Krill then forwarded his wire receipt (which he entitled "Wire Transfer Graham Confirmation $40,000 7 20 15") to Murray, who forwarded it to Rossey. As described above, Rossey made this transfer to Krill, Murray, and Graham, because he was told he was investing in a large international business transaction that never existed.

63. Between May 2015 and August 2016, Krill wired $99,000 from his IOLTA to "Optra Sales and Services Ltd."

64. On April 3, 2015, Krill emailed Murray (at "unite2jaminc@gmail.com") and stated "18,900 wire transfer to Harvey Graham." The attached wire receipt shows a transfer from Krill's IOLTA account to an account with account name "Pey Tradders Ltd."

65. Between May 2015 and August 2016, Krill wired $80,400 from his IOLTA to "Pey Tradders Ltd."

66. On October 17, 2016, "HarveyGraham Solicitors Co" (from account "attorneygraham@hotmail.com") emailed "unite2jaminc@gmail.com" and copied Krill with two sets of bank account information and two dollar amounts. One account/amount combination was "$5,000.00" to an account in England with account name "Andrew Stevens." Nine days later, one of the victims in this case, Gerald Klamrowski, wired $4,000 to Krill's IOLTA and, that same day, Krill wired the $4,000 to the "Andrew Stevens" account identified by Harvey Graham.

67. On February 22, 2017, "HarveyGraham Solicitors Co" (from account "attorneygraham@hotmail.com") emailed "unite2jaminc@gmail.com" and copied Krill attaching a fabricated letter purportedly form the Board of Governors of the Federal Reserve System regarding a financial transaction involving China. The letter is facially illegitimate and includes nonsensical statements like,

> "In line with the laid down principle of the Financial Service Authority (FSA) convey shall be complete swiftly without any hindrances. Upon the approval of the mutually certificated stated above from china is confirmed, there will be no more new certificated required and the beneficiary funds will be credited into his designated account within 24-48 hrs."

68. On January 13, 2016, "HarveyGraham Solicitors Co" emailed a fake letter that purported to be from NatWest Bank to Eric Murray regarding a transfer of funds. Murray then emailed the document to Krill, and Krill forwarded it Rossey on January 14, 2016.

69. On July 5, 2016, Patch wired $8,000 from his company First Pain Care LLC to Krill's IOLTA. The next day, Krill wired $8,000 from his IOLTA to an account with account name "KC Konkwo" and then forwarded his wire receipt, which he named "Wire Graham 7 6 16 $8,000" to "attorneygraham@hotmail.com".

70. In general, an email that is sent to or from a Google or Microsoft subscriber is stored in the subscriber's "mail box" on Google or Microsoft servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google or Microsoft servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's or Microsoft's servers for a certain period of time.

BACKGROUND CONCERNING EMAIL

71. In my training and experience, I have learned that Google and Microsoft provide a variety of on-line services, including electronic mail ("email") access, to the public. Google and Microsoft allow and allowed subscribers to obtain email accounts at the domain name gmail.com and hotmail.com, like the email accounts listed in Attachments A. Subscribers obtain an account by registering with Google and Microsoft. During the registration process, Gmail asks subscribers to provide basic personal information. Therefore, the computers of Google and Microsoft are likely to contain stored electronic communications (including retrieved and unretrieved email for Google and Microsoft subscribers) and information concerning subscribers and their use of Google and Microsoft services, such as account access information, email transaction information, and account application information. In my training and experience,

such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

72. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

73. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

74. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

75. This application seeks a warrant to search all responsive records and information under the control of Google and Microsoft, providers subject to the jurisdiction of this court, regardless of where Google and Microsoft have chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's and Microsoft 's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States. See 18 U.SC. § 2713 (stating in relevant part that "a provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, *regardless of whether such communication, record, or other information is located within or outside of the United States*") (emphasis added).

76. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

77. Based on the forgoing, I request that the Court issue the proposed search warrants. Because the warrants will be served on Google and Microsoft, who will then compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A-1

Property to Be Searched

This warrant applies to information associated with Google accounts unite2jaminc@gmail.com, unityjamii@gmail.com, jonesvillerealtyfinance@gmail.com, and paradise.quest.sm52@gmail.com that is stored at premises controlled by Google, a company that accepts service of legal process at 1600 Amphitheatre Parkway in Mountain View, California.

ATTACHMENT A-2

Property to Be Searched

This warrant applies to information associated with the Microsoft account "attorneygraham@hotmail.com" that is stored at premises owned, maintained, controlled, or operated by the Microsoft Corporation, a company that accepts service of legal process at Online Services Custodian of Records, Microsoft Corporation, One Microsoft Way in Redmond, Washington.

ATTACHMENT B-1

Particular Things to be Seized

I. Information to be disclosed by Google (the "Provider")

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A, for the time period of January 1, 2014 to the present:

a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;

f. All communications, in whatever form, and other information from Google Hangouts associated with the account;

g. All information and documents from Google Docs associated with the account;

h. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Google; and

i. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within fourteen days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 1343 and 1349, those violations involving Michael Krill, Eric Murray, Harvey Graham, Wanda Collier, Noami Ratinov, individuals going by those names as aliases, and others unknown to law enforcement and occurring after January 1, 2014, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Communications between Krill, Murray, Graham, Collier, Ratinov, and their co-actors and victims in furtherance of their scheme to defraud their victims.

(b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the persons who created or used the user ID, including records that help reveal the whereabouts of such persons.

(e) Files and records that contain financial information, credit card numbers, social security numbers, bank account numbers, and other personal identifiable information;

(f) The identity of the persons who communicated with the user ID about matters relating to the scheme to defraud described above, including records that help reveal their whereabouts.

ATTACHMENT B-2

Particular Things to be Seized

I. Information to be disclosed by Microsoft (the "Provider")

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A, for the time period of January 1, 2014 to the present:

j. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

k. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

l. The types of service utilized;

m. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

n. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;

o. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Microsoft; and

p. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within fourteen days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 1343 and 1349, those violations involving Michael Krill, Eric Murray, Harvey Graham, Wanda Collier, Noami Ratinov, individuals going by those names as aliases, and others unknown to law enforcement and occurring after January 1, 2014, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Communications between Krill, Murray, Graham, Collier, Ratinov, and their co-actors and victims in furtherance of their scheme to defraud their victims.

(b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the persons who created or used the user ID, including records that help reveal the whereabouts of such persons.

(e) Files and records that contain financial information, credit card numbers, social security numbers, bank account numbers, and other personal identifiable information;

(f) The identity of the persons who communicated with the user ID about matters relating to the scheme to defraud described above, including records that help reveal their whereabouts.